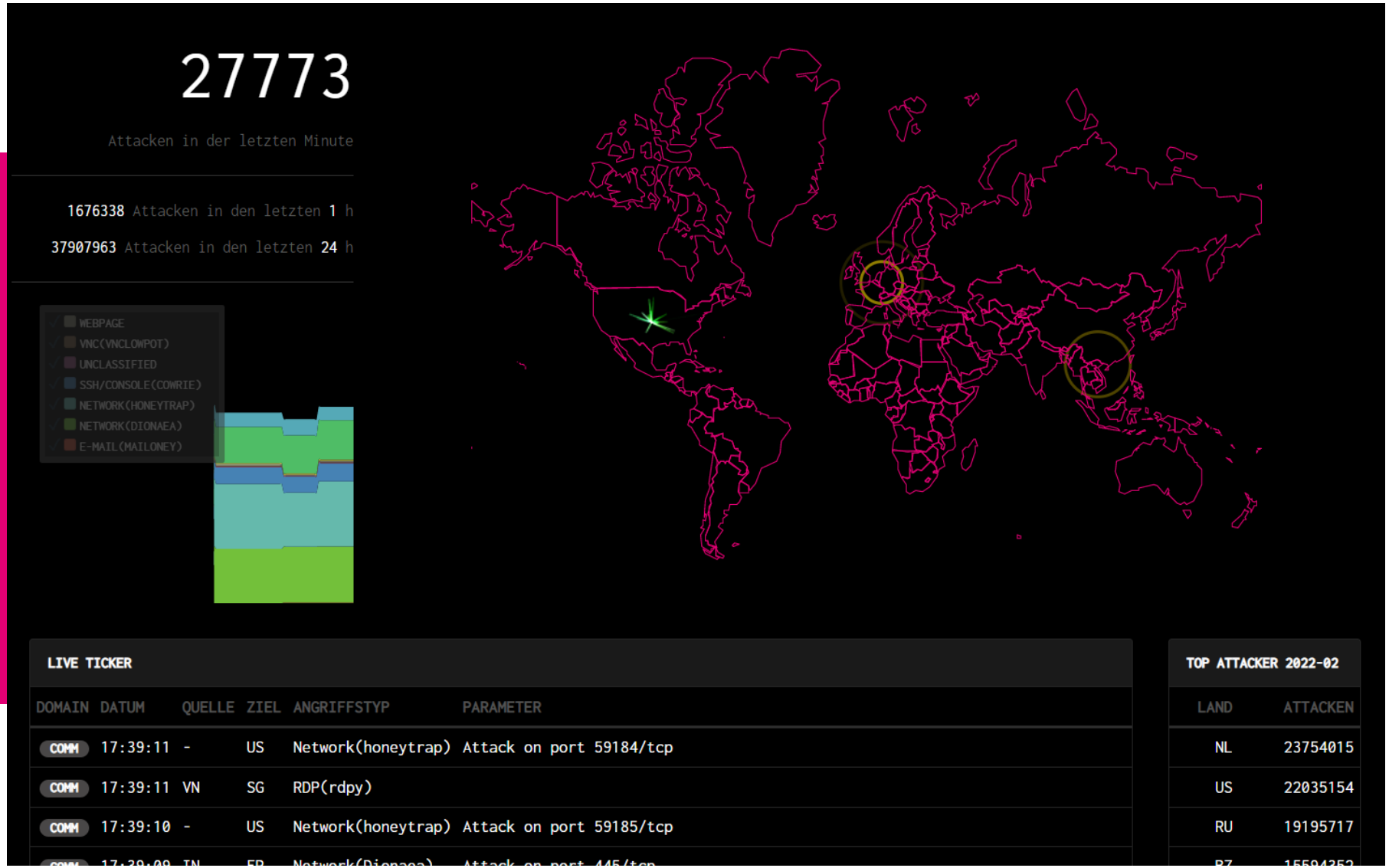
Aktuelle Cyber Lage

Dr. Rüdiger Peusquens, Frankfurt, 27.04.2023

Ein Sturm an Cyber Angriffen

- automatisierte Angriffe
- kurze Zeit, bis Schwachstellen ausgenutzt werden
- erst hacken, dann ausschlachten
- Bots greifen Infrastrukturen an
- zunehmend IoTs als Quellen

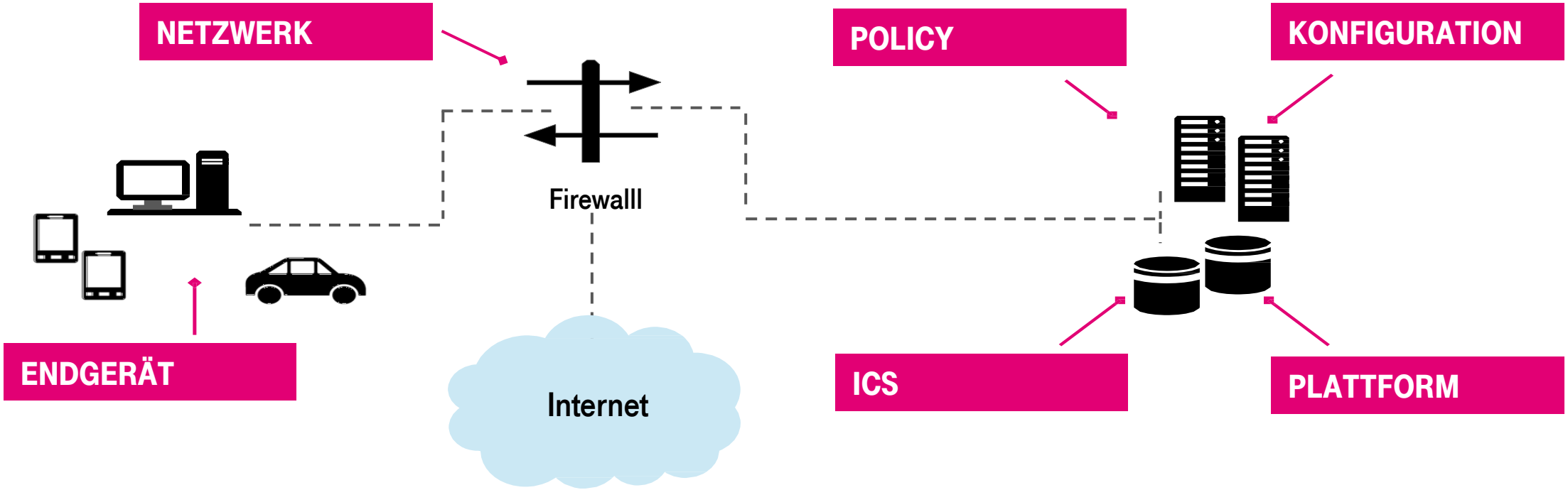
Honeypot Sensoren vermessen Cyber Angriffe
sicherheitstacho.eu



Es geht uns an!
because we...

Digitalisierung ist heterogen und komplex

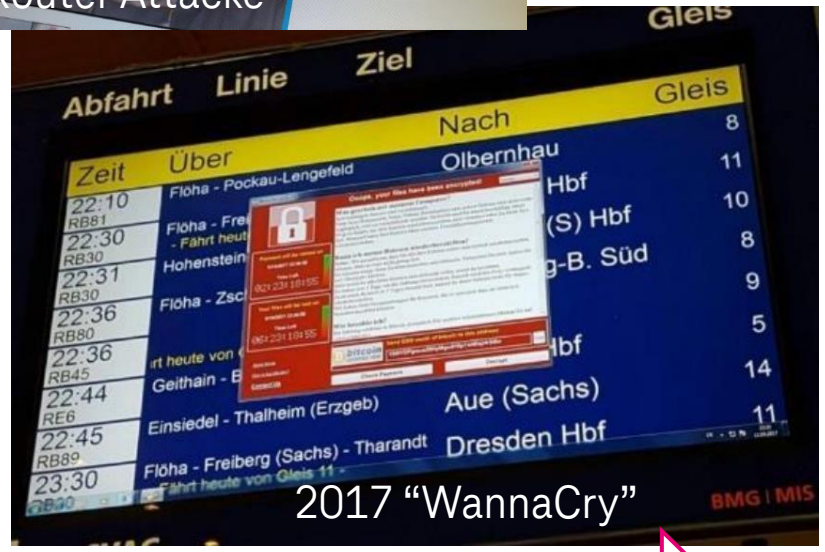
Industry 4.0 | Smart Grid | IoT | Home Automation | Cloud | Autonomous Cars | Health Care



Cyber Crime ist eine Industrie

Cyber damals

2016 “Mirai” Router Attacke



2017 “WannaCry”

Cyber heute

Office of CYBERSECURITY, ENERGY SECURITY, EMERGENCY RESPONSE

Colonial Pipeline Cyber Incident

Office of Cybersecurity, Energy Security, and Emergency Respons

Office of Cybersecurity, Energy Security, and Emergency Response »

Colonial Pipeline Cyber Incident

On May 7, 2021, the Colonial Pipeline
shut down its pipeline system in re
attack. On May 13, 2021, Colonial Pip

ABO SHOP AKADEMIE JOBS MEHR ▾ E-PAPER AUDIO APPS ARCHIV MERKLISTE ANMELDEN

ZEIT ONLINE

Suche

Politik Gesellschaft **Wirtschaft** Kultur ▾ Wissen Gesundheit ▾ Digital Campus ▾ Sinn Arbeit ZEITmagazin ▾ mehr ▾

Oiltanking

Cyberangriff legt Tankstellenzulieferer lahm

Wegen eines Hackerangriffs können insbesondere in Norddeutschland mancherorts keine Tankwagen befüllt werden. Treibstoff gibt es für Kunden

tegut... Gute Lebensmittel

F+ PODCASTS BLOGS THEM

Rhein-Main › Wirtschaft › Software AG

Sonderseite: Coronavirus

Politik Wirtschaft Finanzen

IT-Störung - tegut... Ziel eines Cyberangriffs

Unbekannte haben einen sogenannten Cyberangriff auf das IT-Netzwerk des Unternehmens verübt. Sämtliche IT-Netzwerksysteme der Zentrale sind daraufhin gemäß Notfallplan heruntergefahren und vom Netz genommen worden. Der tegut... Krisenstab hat die Sicherheitsbehörden informiert und arbeitet mit IT-Experten aktuell mit Hochdruck daran, den Normalbetrieb wieder herzustellen.

Wir bedauern diese Unannehmlichkeiten sehr und freuen uns darauf Ihnen bald wieder alle Services und Leistungen vollumfänglich bieten zu können. Vielen Dank für Ihr Verständnis!

NACH HACKERANGRIFF

Software AG ist wieder am Netz

VON INGA JANOVIĆ - AKTUALISIERT AM 23.10.2020 - 10:37

2016/17 gestreut ungerichtet selbstpropagierend

gezielt gut vorbereitet infiltrierend 2020er

Cyber Space ist Militärgebiet

Cozy Bear APT29 FSB

Ziel: Spionage, Inflitration

- SolarWinds supply chain 2020
- COVID-19 Impfstoff 2020
- Republikaner 2021

Fancy Bear APT28 GRU 26165

Ziel: Spionage, Regimegegner

- Bundestag 2014
- Ukraine Artillerie D-30 Howitzer 2016
- Mikhail Khodorkovsky, Maria Alekhina, Pussy Riot
- TV5Monde 2017
- Parlament Norwegen 2020

Lazarus APT38 Generalbüro für Aufklärung

Ziel: Spionage, Sabotage, Betrug

- Sony Datendiebstahl 2014
- Bangladesh Bank 81mio $ Raub 2016
- WannaCry 2017
- Rheinmetall, Renk AG Spionage 2020
- 570mio € Ethereum Diebstahl 2022
- Energieversorger 2023
- W3C VoIP Telefonie 2023

Sandworm GRU 74455

Ziel: Industrial Control Systems

- Ukraine Stromversorgung 2015, 2020
- NotPetya 2017
- Active Directory wiper 2023

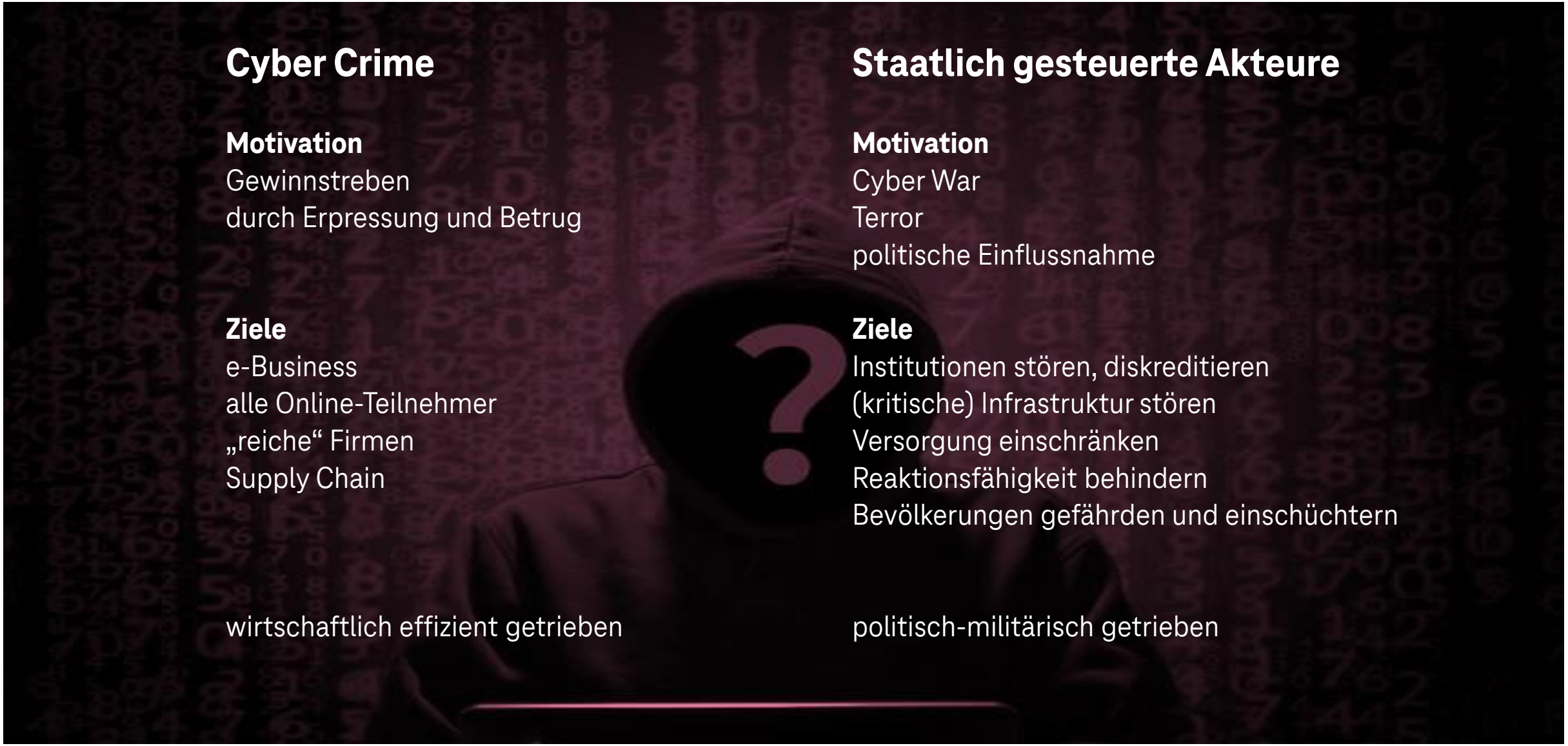
Digitalisierung ist klasse, aber

> CRIME FOLLOWS BUSINESS

> CYBERSPACE IST DIE 4. MILITÄRISCHE DIMENSION

Cyber Crime und staatliche Akteure nutzen gleiche Angriffswege.

Was verfolgen die Angreifer?



Cyber Crime

Motivation
Gewinnstreben
durch Erpressung und Betrug

Ziele
e-Business
alle Online-Teilnehmer
„reiche“ Firmen
Supply Chain

wirtschaftlich effizient getrieben

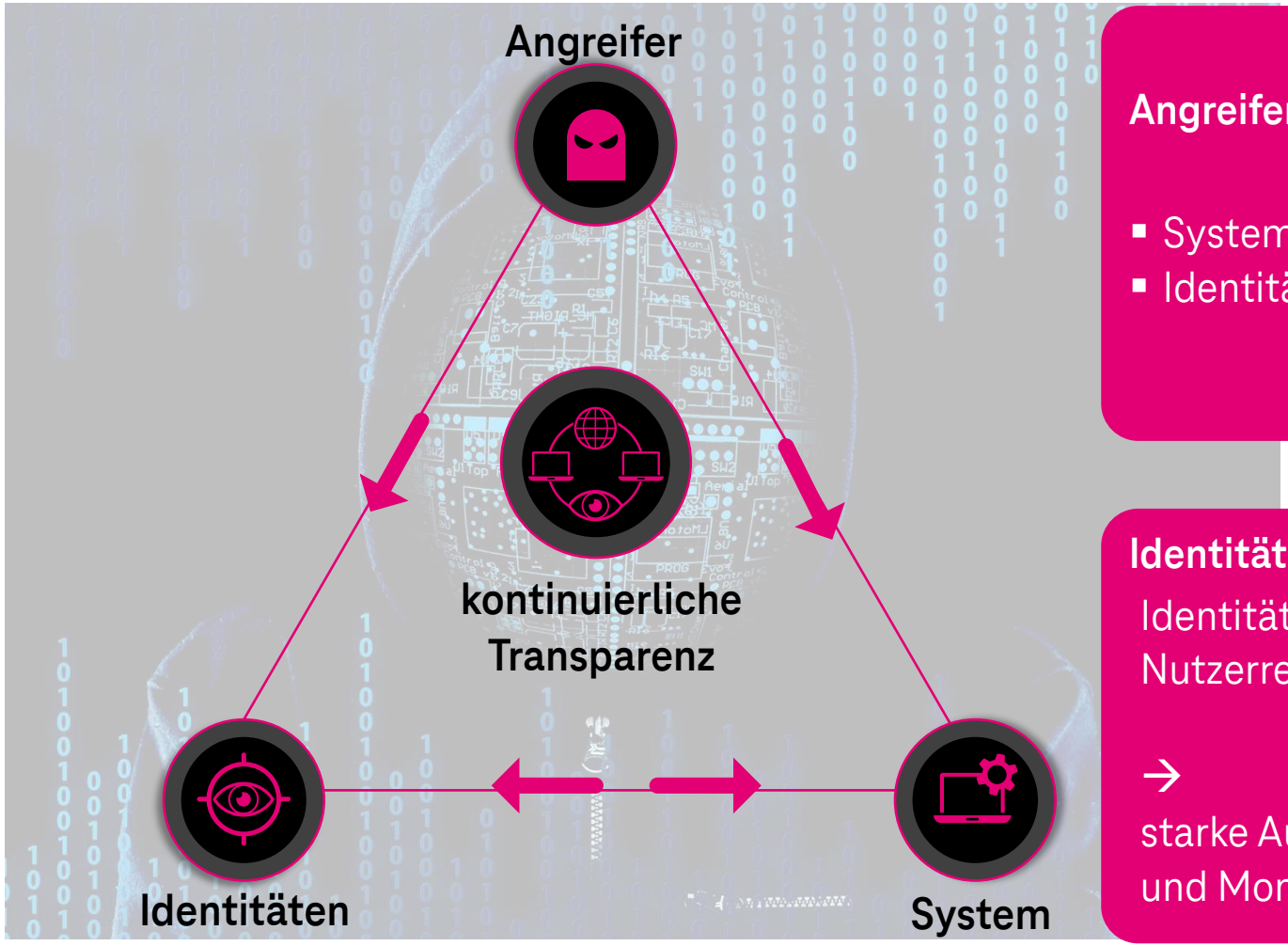
Staatlich gesteuerte Akteure

Motivation
Cyber War
Terror
politische Einflussnahme

Ziele
Institutionen stören, diskreditieren
(kritische) Infrastruktur stören
Versorgung einschränken
Reaktionsfähigkeit behindern
Bevölkerungen gefährden und einschüchtern

politisch-militärisch getrieben

Cyber Defense Dreieck: Wie gehen Angreifer vor?



Angreifer zielen auf

- Systeme
- Identitäten

Systeme

Schwachstellen, Config-Fehler
Fokus: Endpoints
→
kenne deine Infrastuktur, aktualisiere und prüfe

Identitäten

Identitätsklau = Nutzerrechte

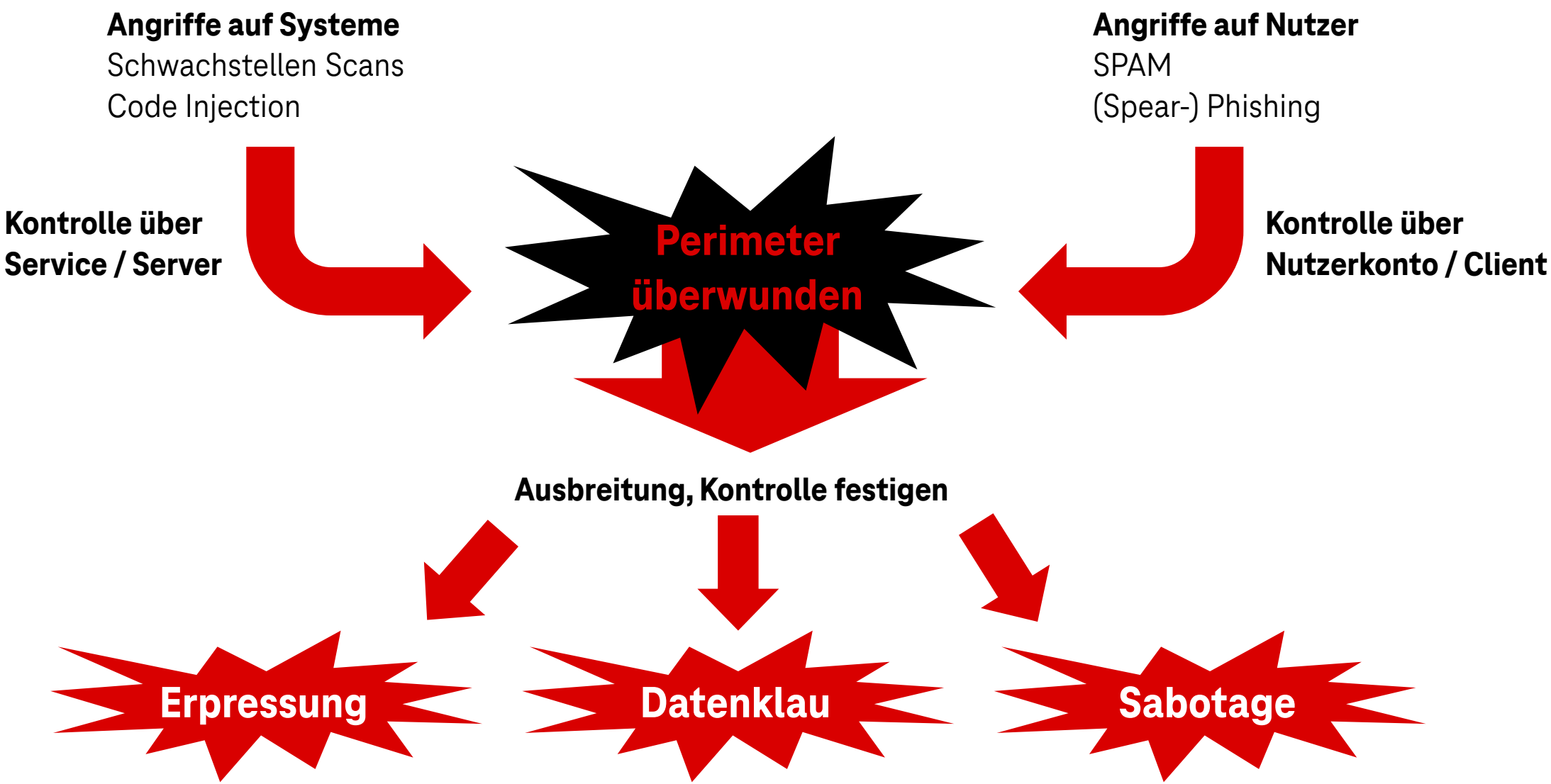
→
starke Authentisierung und Monitoring

Transparenz

Risiken schnell erkennen, effektiv bekämpfen

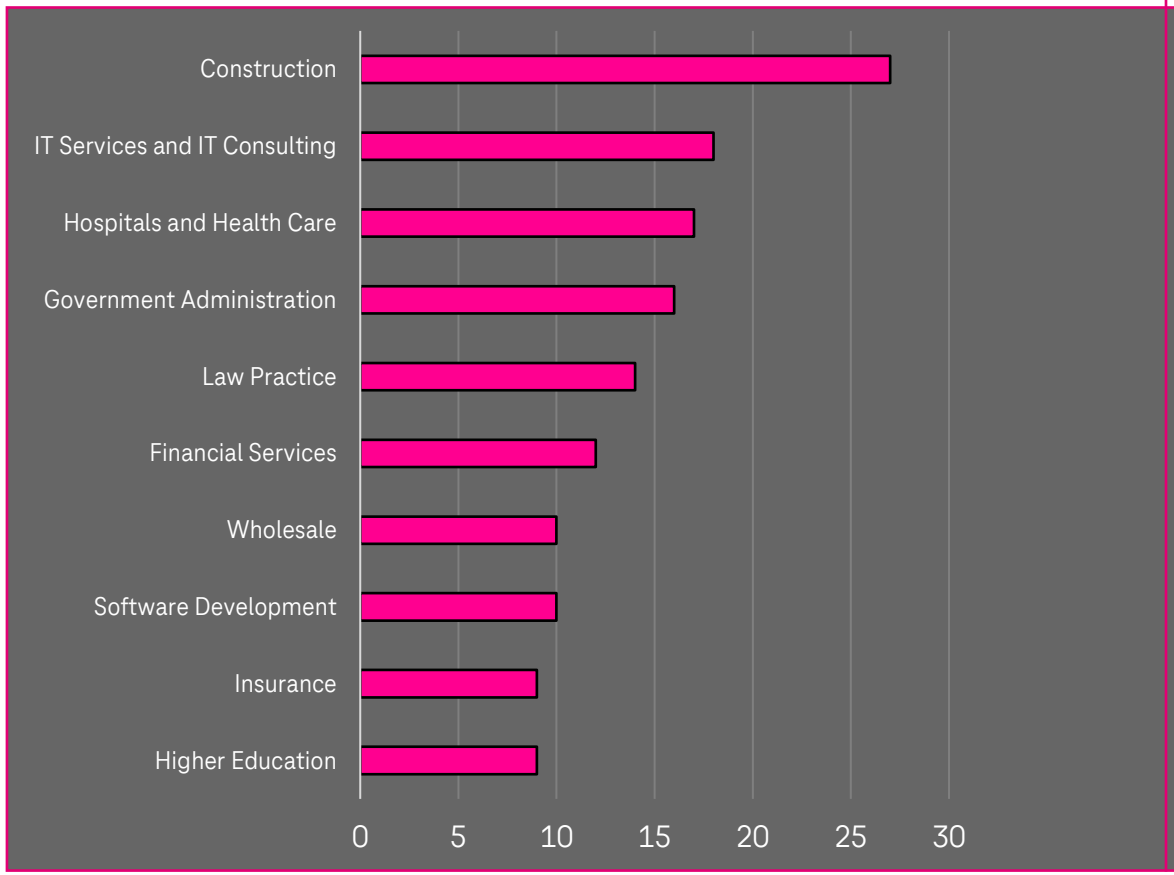
→
7x24 Monitoring, kontinuierlich testen

Grundzüge eines Cyber Angriffs

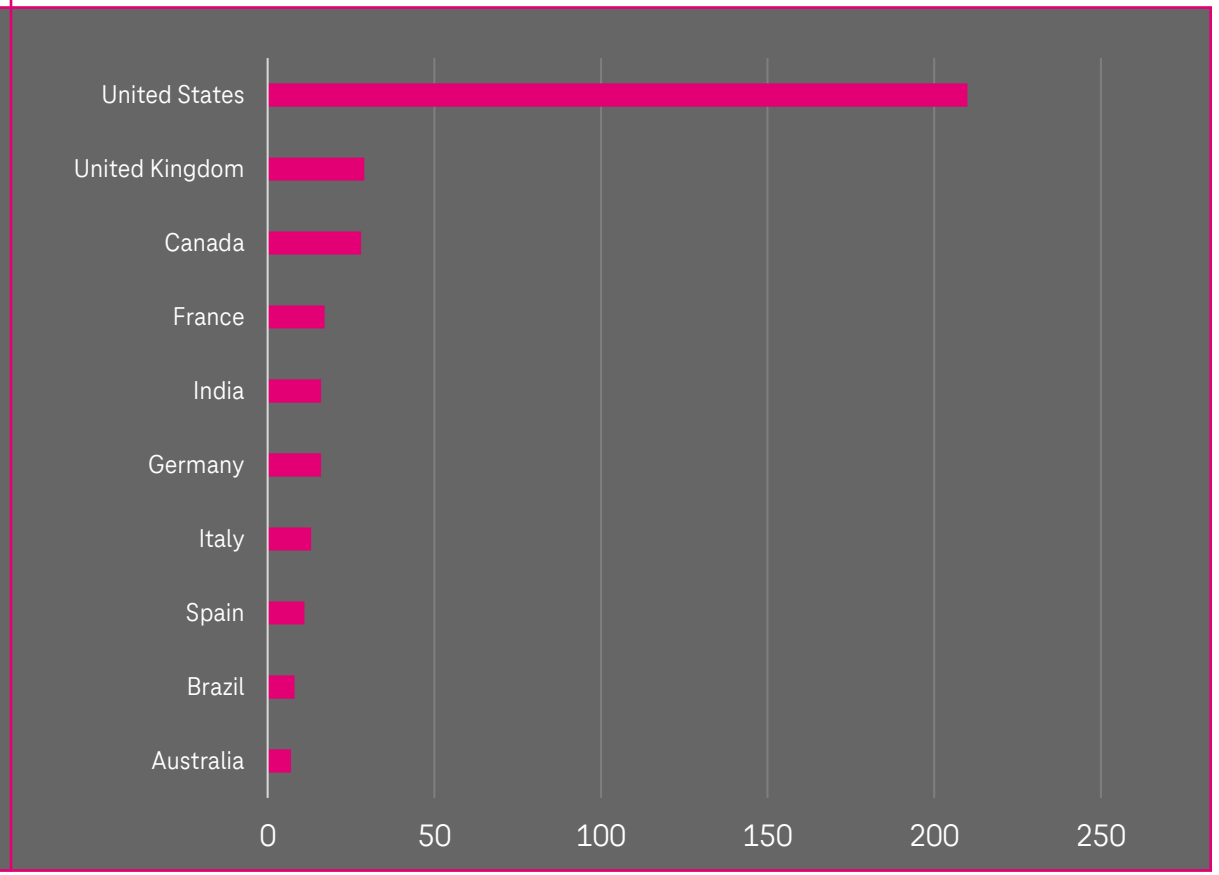


Ransomware Trends: Wen trifft es?

Angegriffene Sectoren*:



Angegriffene Länder*:



* gezählt nur bei klarer Attribution

Angriffe gegen Kunden-Konten

1. Email-Konto des Kunden wird gehackt.
2. Angreifer übernimmt Email-Adresse.
3. Angreifer durchläuft ‘Passwort vergessen’ Prozess. (hier: ebay)
4. Rücksetz-Code geht an übernommenes Email-Konto.
5. Angreifer kann Service-Konto (hier: ebay) übernehmen.

43 Mrd gestohlene Nutzerkonten im Darknet

Angriffe gegen Kunden-Konten

Auf viele Services anwendbar. (hier: facebook)

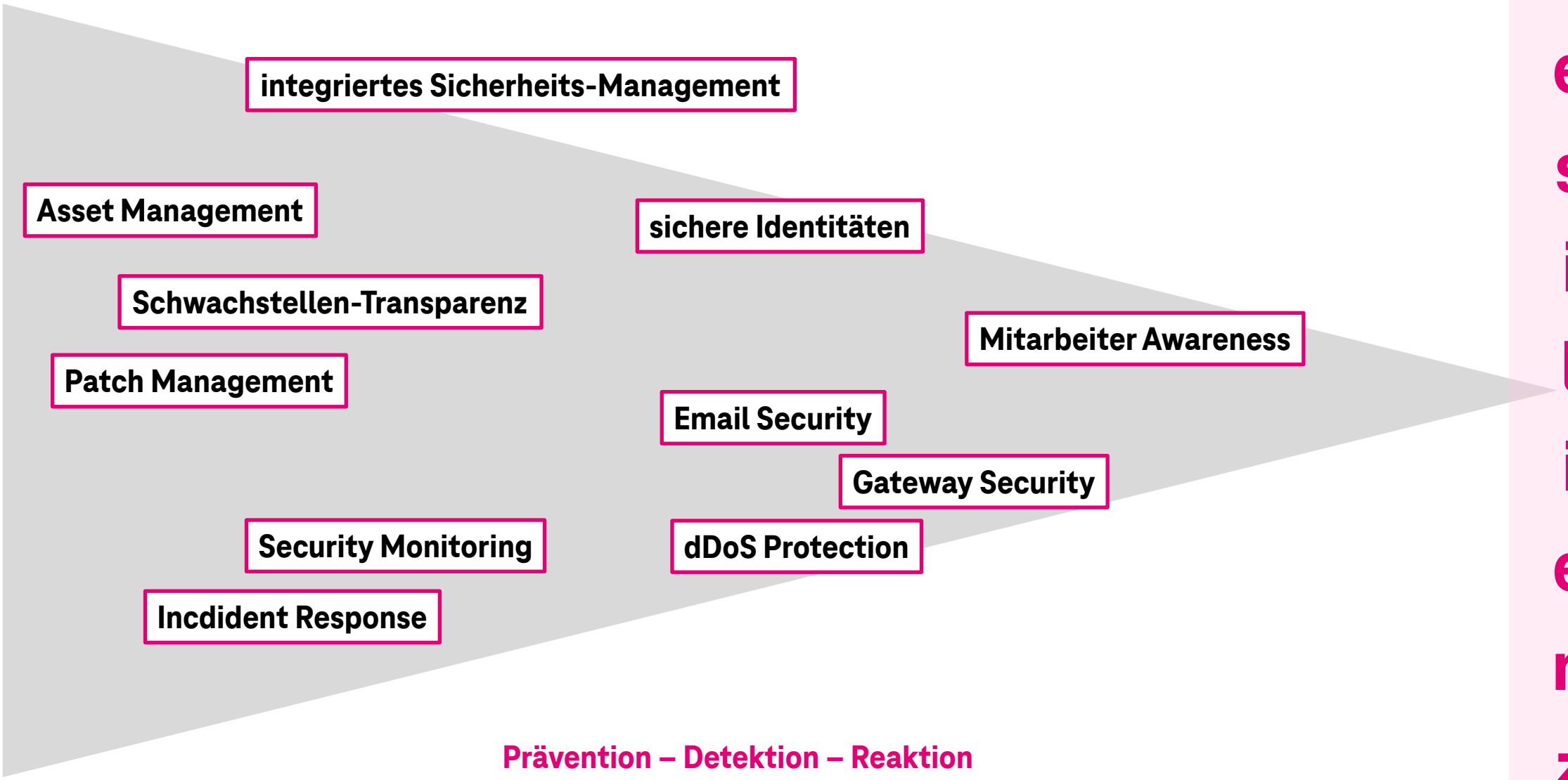
Facebook wird teilweise zur Anmeldung bei Diensten genutzt.

Weiterer Missbrauch folgt.

Blick in eine gehackte Mailbox

Fri 24.02.2023 19:10	Facebook	Hast du dich von einem neuen Ort aus bei Facebook angemeldet?
Fri 24.02.2023 18:56	Facebook	820377 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:52	Facebook	03541415 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:47	Facebook	73831243 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:43	Facebook	70765921 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:42	Facebook	91473114 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:38	Facebook	76339164 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:37	Facebook	76339164 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:34	Facebook	81951441 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:32	Facebook	91448345 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:28	Facebook	88022203 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:22	Facebook	55045025 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:21	Facebook	167758 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:20	Facebook	61140545 ist dein Wiederherstellungscode für dein Facebook-Konto
Fri 24.02.2023 18:17	Facebook	Hast du gerade deine E-Mail-Adresse entfernt?
Fri 24.02.2023 18:17	Facebook	Handlung erforderlich · Schließe jetzt die Sicherheits-Checks ab
Fri 24.02.2023 18:13	Facebook	Hast du gerade dein Passwort geändert?
Fri 24.02.2023 18:10	Facebook	Hast du gerade eine E-Mail-Adresse hinzugefügt?
Fri 24.02.2023 18:00	Facebook	Deine letzte Facebook-Anmeldung
Fri 24.02.2023 17:59	Facebook	35450995 ist dein Wiederherstellungscode für dein Facebook-Konto
Thu 23.02.2023 11:34	Facebook	Deine letzte Facebook-Anmeldung
Thu 23.02.2023 11:33	Facebook	40766029 ist dein Wiederherstellungscode für dein Facebook-Konto

Typische Schutzmaßnahmen



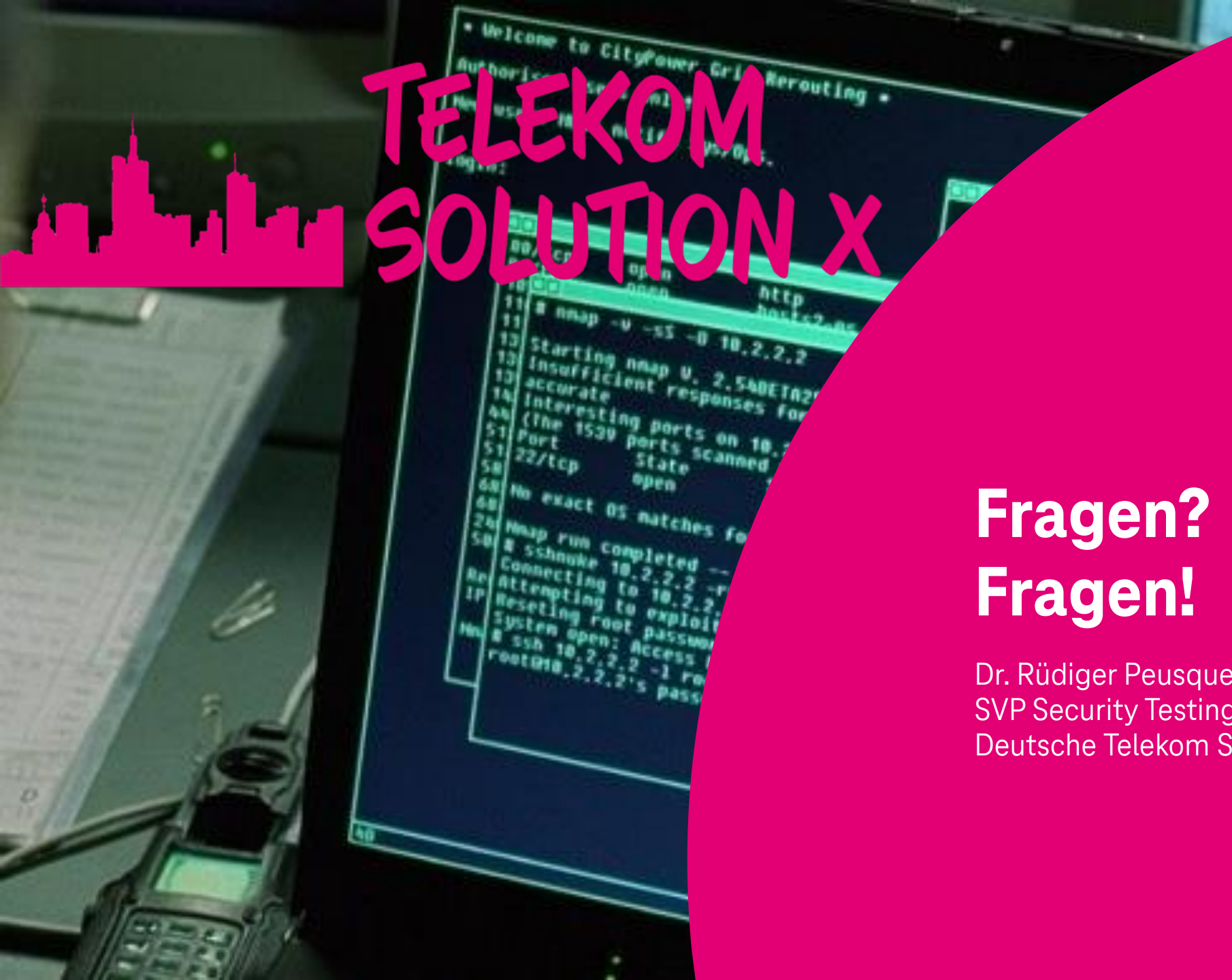
Resilienz

Take Away – Kernaussagen zum Mitnehmen

1. Wir alle sind Ziel von Cyberangriffen.

2. Der Angriffsdruck wächst insbesondere durch staatlich gesteuerte Akteure.

3. Cyber Resilienz ist machbar.



Fragen?
Fragen!

Dr. Rüdiger Peusquens
SVP Security Testing
Deutsche Telekom Security GmbH